APPENDIX 5

END-USE MONITORING OF DEFENSE ARTICLES AND DEFENSE SERVICES

Table of Contents

Forward

End-Use Monitoring has come under increasing scrutiny in the past year as a mission of great importance but also one that receives very little attention. In an August, 2000 report to the Chairman of the House Committee on International Relations, the General Accounting Office (GAO) a number of weaknesses in existing program (GAO/NSIAD 00-208). The report focuses specifically on weaknesses in DoD's program for end-use monitoring noting a lack of specific observation and reporting requirements, ineffective implementation of end-use checks, and lack of guidance or procedures for end-use check standards. Therefore, as of the time of this writing, DoD's End-Use Monitoring program is being thoroughly reviewed for revision. DoD expects to issue revised policy guidance by the end of fiscal year 2001 but in the meantime, interim adjustments will be made. Among those adjustments, DSCA requires Unified Commands, and SAOs, and service security cooperation International Program Offices to identify a single point of contact for end-use monitoring issues. Until DSCA issues further policy, the information provided in this chapter, particularly that concerning post-delivery checks, remains valid.

As a major arms exporter and as a leader in worldwide arms control initiatives, the U.S. has special responsibilities related to control of U.S.-origin defense items. Of all responsibilities associated with management of military articles and services, none is more important than ensuring items are used to further the security of the United States, its friends, and its allies. The continual challenge of meeting this responsibility grows as the variety and sensitivity of items increases. Precautions, developed carefully and refined through decades of experience, are taken to provide items only to countries and international organizations with the capability and the will to assure their full protection and use as prescribed in pre-transfer agreements.

As with other aspects of national security, both for the U.S. and countries receiving sensitive U.S. defense articles or information, end-use monitoring permeates aspects of most actions. Unlike actions which have a beginning and a conclusion, security is persistent and continuous. An effective security process may become so familiar and routine as to operate almost automatically, in virtual obscurity. Those responsible for one part often do not see other parts which, together, provide controls throughout an item's life. This may be optimal for those intimately familiar with the workings of security assistance programs. It is proving inadequate for those only marginally familiar with U.S. processes, who seek to know that controls provide reasonable assurance items will be used only for the intended purposes, misuse will be detected, and any weakness of control will be found and corrected.

This chapter is to highlight key aspects of security measures, to remind us of their importance, to serve as a training media for personnel associated with item security, and to provide a window into our processes to help assure those outside the security assistance structure that appropriate controls exist. It is expected to be of interest to U.S. and country representatives, to help ensure controls are mutually supportive, with minimal duplication and no gaps, to protect the security of both parties.

This chapter is also to provide information related to accounting for items provided to other countries under FAA and AECA programs. It is for use by security assistance offices, program implementing agencies, and others involved in actions related to AECA and FAA endues and retransfer compliance. Should information herein conflict with the *Security Assistance Management Manual*, DoD 5105.38-M, or other official guidance document, guidance in those documents should be followed.

END-USE MONITORING
OF DEFENSE ARTICLES AND DEFENSE SERVICES

Background

Public Law 104-164, signed into law 21 July 1996, established a new Section 40A to the Arms Export Control Act (AECA). Extracts from the new law are as follows:

- In order to improve accountability with respect to defense articles and defense services sold, leased, or exported under the AECA or the Foreign Assistance Act of 1961 (FAA), the President shall establish a program which provides for the end-use monitoring (EUM) of such articles and services.

- To the extent practicable, such program shall provide for the EUM of defense articles and defense services in accordance with the standards that apply for identifying high risk exports for regular end-use verification developed under AECA, Sec 38(g)(7), commonly referred to as the Blue Lantern program. The program shall be designed to provide reasonable assurance the recipient is complying with the requirements imposed by the U.S. Government (USG) with respect to use, transfers, and security of defense articles and defense services and such articles and services are being used for the purpose for which provided. The Foreign Relations Act for FY 2000/01 (P.L. 106-113, 29 Nov 99) further addressed the issue of verification. Specifically, it now requires that any agreement for sale or lease of any article on the United States Munitions List made after 29 Nov 99 state that the USG retains the right to verify credible reports that the article(s) has been use for a purpose not authorized under Section 3 of the AECA.

- The program must provide for the end-use verification of defense articles and services that incorporate sensitive technology, that are particularly vulnerable to diversion or other misuse, or where diversion or misuse could have significant consequences. The program must also prevent diversion, through reverse engineering or other means, of technology incorporated in defense articles.

- An initial stand-alone report as well as annual reports within the Department of State (DoS) Congressional Presentation (CP) are required. The information which follows shows new steps as well as existing policies and practices which implement the above legislation. Taken together, they are designed to provide a level of accountability assurance at least equal to that of the Blue Lantern program, which is a major objective of the new legislation.

Blue Lantern

Blue Lantern is a U.S. Department of State (DoS) program. Initiated in 1990, the program is directed toward verifying end-use of commercial defense trade. Its primary purpose is to ensure defense articles, defense services, and related export data are exported in compliance with the AECA.

Blue Lantern provides pre and post-shipment checks during the defense articles and services export process. Pre-shipment checks generally verify that planned transactions are accurately and completely reported to DoS and item shippers and recipients are as represented on export documentation. Post-shipment checks generally ensure items were received by the approved entity and are being used in accordance with the terms of each DoS approval. The Blue Lantern program has established a list of 20 key warning flags for identifying high risk exports.

Meeting Blue Lantern Standards

AECA, Sec 40A requires AECA and FAA government-to-government programs to meet Blue Lantern standards. Defense articles and services are provided under the AECA and FAA for internal security, self-defense, civic action, or for other use in accordance with agreements to which the USG and country are parties. Blue Lantern screening of AECA commercial actions based on DoS problem indicators/catalysts for export checks is intended to reduce the possibility for any other use of these items. It is also intended to prevent use by anyone other than the party specified on an approved defense export license.

The Blue Lantern standards (problem indicators/catalysts for end-use checks), with corresponding government controls which provide equivalent end-use assurances for government-to-government programs, are as follows:

Customer

1.a Blue Lantern Customer or purchasing agent is reluctant to provide foreign endues or end-user information.

1.b Government Controls A Presidential Determination (see Annex B) must be in place (FAA, Sec 503(a) /AECA, Sec 3(a)(1)) authorizing AECA and FAA programs with the potential item recipient. DoS must have approved each sale (AECA, Sec 2). Generally, the U.S. Department of Defense (DoD) may sell only to its defense equivalent, including military services, within the recipient country. Government-to-government programs will not proceed, and item delivery will not occur, if any end-use or end-user questions are not resolved.

2.a Blue Lantern Customer is willing to pay cash for high value orders, or to provide unusual or extremely lucrative financial compensation for the product.

2.b Government Items are purchased for AECA transfers (Foreign Military Sales, or FMS) using funds deposited in advance. The U.S. originally purchased for itself those items granted to foreign countries under the FAA. In both scenarios, the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) are used, with very restrictive purchase rules which are virtually identical to those for acquisition to supply USG, including DoD, requirements.

3.a Blue Lantern Customer's business background information is scanty or unavailable.

3.b Government A Presidential Determination that indicates programs with a given country will strengthen U.S. security and promote world peace is the first formal step for AECA and FAA programs with a country. Analyses leading to the determination consider the country's general ability and willingness to protect hardware or information subsequently provided equivalent to that which is provided by the United States. Additional controls, with more stringent controls imposed for more sensitive items, will be discussed later in this chapter. Unlike commercial firms, the country is a known quantity prior to consideration of the first, normally relatively small, program. This familiarity increases as successively more complex programs are developed.

4.a Blue Lantern Customer appears unfamiliar with the product or its application, performance/design characteristics, support equipment, or uses.

4.b Government To ensure an item meets the requirement, initial discussions, and early planning provide information so the country is aware of general item capabilities and support requirements. Complex items are normally provided by DoD with a support package which includes training, publications, and other technical support. Government programs are able to emphasize long term cooperation. DoD works with customer country representatives in AECA/FAA and non-security assistance programs, such as joint exercises, over long periods of time. This normally provides a means, when it serves U.S. interests, to gain familiarity with U.S. defense items.

5.a Blue Lantern Customer declines service, installation, warranty, spares, repair, or overhaul contracts that are normally accepted in similar transactions.

5.b Government Acceptance or non-acceptance of these items is reconciled during pre-program planning. The country's acceptance/rejection decision is often consistent with a DoD recommendation, or made following consultation with DoD. DoD is aware, with relatively high certainty, why parts of programs are accepted or rejected.

6.a Blue Lantern Customer orders products or options that appear to be incompatible with the customer's environment or line of business.

6.b Government These factors are normally considered during pre-program planning, along with larger issues such as precedent which could lead to similar requests from other countries, technical and economic ability to operate and maintain the item, and compatibility with other country force structure.

7.a Blue Lantern Customer provides vague delivery dates or delivery locations/instructions that are inconsistent with either the type commodity or established practices.

7.b Government DoD establishes the delivery dates for FAA and AECA programs. The point of delivery is approved in advance through a formal process, with increasing security levels as the sensitivity of a given item increases.

End-User

8.a Blue Lantern Requested equipment does not match the known requirements or current inventory of foreign end-user.

8.b Government The U.S. in-country team, led by the Ambassador, is aware of FAA and AECA programs with the country. Major programs are normally discussed with country representatives and within the U.S. security assistance community prior to implementation, to evaluate courses of action and ensure programs fit into U.S.-country planning.

9.a Blue Lantern Requests for spare parts are in excess of projected needs or are for systems not in the foreign end-user's inventory.

9.b Government Spare parts packages in conjunction with major equipment sales are normally defined based on U.S. recommendations. Recommendations are based on DoD experience, including U.S. and foreign programs involving the system at issue or similar systems. The country normally works with the U.S. to adjust the quantities based on factors such as spares already on hand or the in-country part failure experience. Spare parts sales agreements restrict sales to parts applicable to certain end items. These procedures restrain any inclination to purchase unauthorized parts.

10.a Blue Lantern Performance/design requirements are incompatible with the foreign end-user's resources or environment.

10.b Government The model of any weapon system to be provided is a substantial and integral part of pre-program analyses within the DoS-DoD sale approval coordination process. The intended recipient is known, and U.S. willingness to release the requested item receives careful attention. Higher lethality, higher technology, and other particularly sensitive items receive the greatest scrutiny.

11.a Blue Lantern Stated end-use is incompatible with the foreign consignee's line of business or with the technical capability of the foreign consignee or foreign end-user.

11.b Government Release of the defense article or service will be only to the country's defense establishment, including pre-approved agents such as a verified freight forwarder to manage transportation to the recipient country. When DoS and DoD determine a given item is releasable, the stated end-use (internal security, self-defense, etc.) is seldom an issue. At the point of item release, the country's agreement, assuring end-use will be as authorized by the AECA and FAA, is in place. Technical capability is resolved during program planning or execution, through a decision not to acquire the item, training to overcome deficiencies, or other actions.

12.a Blue Lantern End use information provided is incompatible with standard uses or practices.

12.b Government This is resolved during program execution. For example, training or other technical support may resolve questions of proper deployment and use of the defense articles. The agreement signed by the recipient country prior to program implementation provides the general parameters for allowed end-use or retransfer (see Annex C).

13.a Blue Lantern Orders are placed by firms or individuals from foreign countries other than the country of the stated end-user.

13.b Government An "order" under the FAA or AECA is an approved program, such as represented by an implemented United States Letter of Offer and Acceptance (LOA). Items can be provided only to the country which signs end-use, retransfer, and other pre-program agreements with the United States (see Annexes C and D). Alternate arrangements would not survive the pre-program coordination process.

14.a Blue Lantern Evasive responses are given to questions regarding any of the above, as well as to whether the equipment is for domestic use, export, or re-export.

14.b Government Evasive responses would not be accepted. Specific actions and information are required in order to implement a program under the FAA or AECA. For example, a specific statement regarding restrictions on equipment use is included in each LOA in accordance with AECA, Sec 3(a). Similar agreements are executed within each grant transfer in accordance with FAA, Sec 505(a).

Shipment

15.a Blue Lantern A private intermediary is involved in the export, particularly in sales involving major weapon systems.

15.b Government Private intermediaries, such as freight forwarders arranging transportation from the U.S., become country agents and are formally incorporated into

government programs. For example, freight forwarder facilities must undergo investigations and inspections before being cleared by DoD for transshipment of classified items. Freight forwarder addresses are included in the Military Assistance Program Address Directory (MAPAD), along with information showing types of shipments which each freight forwarder is authorized to handle.

16.a Blue Lantern Customer designates freight forwarders as foreign consignees or foreign end-users.

16.b Government The attempted designation would be rejected. Each FAA or AECA program is based on a formal agreement with the recipient country. The agreement includes the proper end-use of the items and rules for retransfer. U.S. representatives implementing these programs are aware, and country representatives would be informed, that freight forwarders are not authorized end-users.

17.a Blue Lantern Customer uses foreign intermediate consignee(s) whose location or business appears incompatible with the purported foreign end-user's business or location.

17.b Government Any use of foreign intermediate consignees is carefully reviewed but may be approved under specific circumstances. For example, a low technology item might be delivered to the North Atlantic Treaty Organization's (NATO) Maintenance and Supply Agency (NAMSA) for application of a modification prior to final movement to the recipient country.

18.a Blue Lantern Customer gives instructions to make direct shipments to trading companies, freight forwarders, export companies, or companies with no apparent connection to the purchaser.

18.b Government This would be noted during program execution and alternate, approved, shipping arrangements would be made.

19.a Blue Lantern Customer requests packaging requirements that are inconsistent with shipping mode and/or destination.

19.b Government DoD determines packaging requirements for FAA and AECA programs. This is due to mutual interest in adequate protection in order to meet each requirement with minimal damage and cumbersome discrepancy resolution. While the customer country may request and justify alternate packaging, this almost never occurs.

20.a Blue Lantern Customer chooses circuitous or economically illogical routing, such as through multiple countries or companies.

20.b Government Indirect routing to the end-user is sometimes required in order to take advantage of carrier availability. Transportation of classified and other sensitive items is normally arranged by DoD in order to ensure en route security. When DoD does not arrange transportation of a sensitive item, a transportation plan is coordinated between DoD and the recipient country to ensure controls are comparable to those which would be provided by DoD.

DOD GOLDEN SECURITY PROGRAM

The DoD end use monitoring program, covering defense articles and services transferred on a government to government basis, will be called the Golden Sentry (GS) program.

Action

SAOs, Service Security Cooperation International Program Offices and unified commands are each requested to provide DSCA with a designated contact (Name of individual, position, title, telephone number, fax number, email — Unclassified and Classified) who will be responsible for oversight of the Golden Sentry ELTM program in-country/at the service level at the unified command and their estimated departure date (If Applicable). As designated officials change, DSCA requests a new POC be designated and DSCA be informed accordingly. Request SAOs / Services / Unifieds provide this information to DSCA by email no later than April 30,2001. End Action.

PROGRAM RATIONALE AND GOALS

DSCA, in the office of Undersecretary of Defense for Policy, Office of Secretary of Defense, is responsible for administering DoD aspects of EUM to include the review of requests for export through purchase or transfer on a government to government basis of defense articles, defense services, and related technical data. Until this time, end-use monitoring of government to government arms exports has been executed largely on a service security assistance program manager program office - led basis. This form of management has been highly responsive in ensuring that DoD makes fully informed government to government export decisions. However, it is increasingly apparent that OSD, through DSCA, must play a more visible role in tying together service efforts into a clear and cohesive EUM program to effectively enforce the Arms Export Control Act (AECA) AND FOREIGN ASSISTANCE ACT (FAA) OF 1961.

Legislation passed in the latter part of 1996 amended the AECA to require the establishment of a comprehensive end-use monitoring program for arms sales and transfers made under the authorities contained in the AECA and the FAA to verify reasonable assurance of recipient compliance with USG export control requirements. The blue lantern program for monitoring of commercially sold USML items, initiated in 1990, constituted a significant portion of the executive branch of response to these legal requirements, as does state department activity to monitor, report, and address unauthorized arms transfers and diversions in accordance with section 3 of the AECA. DOD, on its part in late 1996, published and EUM booklet (see reference) and added specific EUM sections to the Security Assistance Management Manual (SAMM) DOD 5105.38-M. However, the 2000 GAO report on FMS end-use monitoring indicated that additional DoD implementing instructions have not provided the level of necessary guidance to field personnel ostensibly charged with carrying out ELTM duties as part of their assigned mission responsibilities.

U.S. Policy goals supported by the DoD Golden Sentry program include:

- Impeding the access of potential adversaries to military significant items and technologies, including those which contribute to the proliferation of weapons of mass destruction;

- Promoting a capable defense industrial base to ensure global competitiveness and continued technological advantages enjoyed by U.S. military forces over potential adversaries;

- Transfer and end-use of defense equipment and services. ENCOURAGING FOREIGN GOVERNMENT SUPPORT FOR U.S. PRINCIPLES, LAWS, REGULATIONS, AND PRACTICES CONCERNING THE SALE,

It is important to recognize that the DoD Golden Sentry program, for government to government transfers of defense articles and services starts with the bar for higher than for

commercial defense exports. If Golden Sentry finds an unauthorized use or retransfer, it at a minimum, shows carelessness on the part of a government we trusted to be careful. At worst, it is betrayal of an international agreement. DoD EUM monitoring officials on the ground will typically be close contacts of the units being checked. For example, SAO officials may be inventorying the equipment of units they have, are, and/or will be assisting to obtain and integrate equipment, software and training. They will be able to certify end use of equipment from personal observation in the course of other assigned duties rather than making a special representation to the host government.

DSCA will provide further amplification of the Golden Sentry program during the coming months as it takes further shape. Resources, program goals, and methods of operation will be adjusted to match each other as the program develops. The education process will start once Golden Sentry EUM POCs are identified to DSCA.

DSCA point of contact for the Golden Sentry end-use monitoring program is Brion Midland/DSCA/Policy, Plans & Programs directorate (P3), DSN 329-3864, commercial (703) 601-3864, unclassified email Brion_Midland@nts.policy.osd.smil.mil.

GOVERNMENT PROGRAM COMPLIANCE WITH AECA, SEC 40A

DoD policy (see SAMM Chapter 6) calls for general neutrality regarding use of governmental or commercial channels for acquiring U.S. defense items. Experience indicates that most commercial programs afford end-use and retransfer controls comparable to those provided through government programs. Primarily due to more experience among managers of government programs, there is greater assurance of a consistent understanding of end-use and retransfer requirements within government channels. A major distinction between commercial and government-to-government program controls lies in the level of USG attention which is routinely given to each program.

Government-to-government programs involve USG representatives from program planning to delivery of items, support of the items during many years of use, and ultimate disposal. SAO (FAA, Sec 515(a)) and other members of the U.S. country team, U.S. commercial interests, and other contacts remain engaged beyond delivery, allowing interface with the user throughout an item's life. These differences are most pronounced during the stages of security assistance programs from preliminary discussion of the requirement to hand-off of the items. Identification of potential weaknesses involving commercial programs has resulted in establishment of standards (warning flags) under the Blue Lantern program in order to partially replicate the more exacting controls routinely exercised within government programs.

Most government program controls are embedded throughout security assistance processes, and are easily taken for granted. Evidence of their existence is seen through study of security assistance legislation, policies, and procedures. They are also shown through AECA, Sec 3 reports to Congress, submitted by DoS based on indications of unauthorized use of items provided under AECA and FAA programs. Even though other countries are using U.S. defense items valued at hundreds of billions of dollars, violations of government program end-use and retransfer agreements have been quite low. One purpose of the program based on AECA, Sec 40A is to continue, or improve, this record.

AECA, Sec 40A provides an opportunity to ensure end-use controls remain a high priority within AECA and FAA programs. This chapter summarizes controls already in place and to be incorporated in guidance such as the Security Assistance Management Manual, DoD 5105.38-M. It is to be a reminder that procedures often have multiple purposes, one being end-use controls.

Procedures incorporating those controls must be thoroughly understood and followed in order to minimize end-use violations.

End use controls within government programs are focused in two areas:

- Authorized item recipients which

- Prove consistently trustworthy of receiving defense articles and services and maintain good interface with the U.S. to provide required protections, especially after delivery. The incentives for protection vary. End user protective measures may stem from knowledge items are also part of a recipient's defense structure and compromise would weaken internal defenses, from a desire to demonstrate trustworthiness within the international community, from an intent to foster or sustain a defense relationship with the United States, or from other sources.

- Maintain good internal accountability for defense items. SAO and other USG representatives assist country representatives to maintain or improve item controls. It is seldom possible for USG representatives to effectively substitute their own actions for in-country accounting controls.

- A system of checks and cross-checks which ensures

- Items are ordered by a country or international organization which is authorized to participate in AECA and FAA programs and has formally agreed to provide required protection for articles or information received,

- Release has been properly cleared within the DoS-DoD coordination process, and

- Delivery is to the proper representative of the ordering country or organization.

The foundation for end-use controls is usually established long before the first defense article or defense service is provided under the AECA or FAA. U.S. relationships with countries evolve from the myriad of U.S. contacts with representatives of each country. The evolution of a typical country program is summarized in Annex E.

SENSITIVE ITEM CONTROL

Certain categories of items provided under AECA and FAA programs are subject to extraordinary controls.

Classified items receive added controls because capabilities or technologies could provide significant advantage to entities whose interests do not coincide with United States national objectives. A breakdown in these controls would present substantial risks which may not be seen for years, and may not then be traceable to a specific source. Negligent release of classified items, including data, is a persistent concern related to the use of classified items within DoD as well as in foreign transfers.

Arms, ammunition, and explosives (AA&E) items receive special handling due to the risk of falling into the hands of terrorist, organized crime, or other elements whose interests are detrimental to U.S. national objectives. Many of these items can also pose an immediate danger to those nearby when unauthorized use occurs.

There are further gradations of control beyond those discussed above. For example, an item may be identified for accountability purposes as pilferable. A pilferable item, such as a bayonet,

is considered to be broadly useful or desirable. These items require higher than routine protection but the impact of any loss is less significant than for classified items or for sensitive AA&E.

Because the dangers are more subtle and the risks more significant, procedures are in place to increase controls over classified items until those items are destroyed or declassified. Experience shows AA&E item risks are more readily understood and countries generally protect these items to avoid repercussions from their own citizenry. DoD therefore applies relatively stringent AA&E controls while items are in U.S. custody and normally reminds the country of additional controls needed once released by the U.S. For example, except as cargo loaded and prepared for departure, recipient countries are seldom allowed to assume control of sensitive AA&E items within the Continental United States. Controls for pilferable items are comparable to those for AA&E, but less restrictive. For example, the bayonets mentioned above might be held at a secure freight forwarder facility until an economical cargo load is consolidated whereas a sensitive AA&E item would be loaded at the airport or seaport and removed without delay from the United States, or transported under U.S. control to the recipient country.

The following are examples of the added controls which apply for classified items:

- General Security of Military Information Agreements (GSOMIAs, see Annex D) are developed and implemented when relationships with other countries reach a stage where release of classified military information is beneficial. This normally occurs before cooperative programs are implemented, including those under the AECA and FAA, and always before sensitive items are released. A GSOMIA is a government-to-government agreement, negotiated through diplomatic channels. It states, in substance, that each party to the agreement will afford to classified information provided by the other the degree of security protection afforded it by the releasing government. It contains provisions concerning the use of each other's information, third party transfers, and proprietary rights. It specifies that transfers of information will be on a government-to-government basis. It provides that both parties agree to report any compromise, or possible compromise, of classified information provided by the other party. Moreover, the GSOMIA states that both parties will permit visits by security experts of the other party for the purpose of conducting an assessment of governmental security programs at both military and defense industrial facilities.

- Under NDP, teams of three or four counterintelligence and security professionals from U.S. member agencies visit recipients. The teams assess the basis for the protection of classified information in the country and determine if the country has the capability to protect U.S. classified military information in a manner that is substantially equivalent to protection afforded by the U.S.

- Security surveys should be updated periodically so they provide a current basis on which national decisions can be made regarding disclosure of classified information. A survey of recipient government security programs every five years is the goal. Significant changes to a recipient country's laws or political leadership or other factors may result in advancing the survey schedule. Under certain circumstances, such as when a mutually acceptable time for a survey cannot be found, the time between surveys might be longer.

- During these security surveys, the team meets with recipient government officials to discuss laws, regulations, directives, practices, and procedures related to personnel security, information and document security, physical security, and industrial security. The team also attempts to learn about the host government's export control laws, regulations, and procedures. In addition, visits are made to military installations (generally one Army, one Navy, and one Air Force) and at least two defense industrial facilities where classified information and equipment are handled.

• While visiting military facilities, the team also checks the status and security of U.S. classified equipment which has been sold to the host government through AECA or FAA programs. This includes inventorying the U.S.-provided equipment on hand.

• A report of team findings is provided to the country team. Information obtained helps in the continuous evaluation of the effectiveness of country security doctrine and procedures.

• Early in the process leading to release of a defense item, analyses are completed to determine if classified hardware or information will be released and to what extent. Classified items are released parsimoniously, to meet the immediate needs within each program. For example, classified information regarding item capabilities or vulnerabilities is normally released late in the program. Countries which receive low item quantities have only small parts of their budget invested and the items are a smaller part of their defense. They are therefore regarded as having less incentive to maintain security controls equivalent to those provided by the United States. For these reasons, low quantity programs are reviewed more carefully to ensure a fully operating control regimen will be employed. Programs involving release of token quantities of one or two classified items are not normally approved.

• Standard terms and conditions (Annex C) within each transfer agreement require the same security controls as the U.S. would provide for itself. Special investigations and inspections are completed, and clearance is granted by DoD, prior to shipment of any classified item through a country freight forwarder. Transportation plans, which show specific controls in each stage of tem delivery, are necessary prior to approving shipment of classified items outside Defense Transportation System channels.

• Classified items receive extra attention from USG intelligence organizations, as well as groups such as the Technology Transfer Working Group (TTWG). The TTWG is made up of senior representatives of intelligence agencies, U.S. Department of Justice, U.S. Department of Commerce, Department of Treasury, DoS, and DoD. It meets regularly to exchange information and plan actions to address problems related to illicit use or transfer of equipment or technology, U.S. and non-U.S., worldwide.

The following, extracted from DoD manual 5100.76-M, “Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives”, are not all inclusive but are illustrative of controls added for sensitive AA&E:

• The most sensitive AA&E items, designated Category I, require two person certification of serial numbers at the point of shipment; sealing and locking of the container in the presence of those individuals; use of DoD-owned, chartered, or approved carriers; and DoD security to the overseas port of debarkation.

• Although required by agreement only for classified items, the country normally provides protection for all U.S.-origin items which is equivalent to that provided by the U.S. This includes all facets of item protection; such as, storage facilities construction and lock specifications, fences and other fixed perimeter security, and timing of guard patrols.

ADDED STEPS TO ENSURE AECA, SEC 40A COMPLIANCE

When an indication of unauthorized end-use is found within a country, checked locally, and not resolved, the country team forwards the information to DoS. Among actions by DoS will be a determination as to whether AECA, Sec 3 criteria for a report to Congress of a possible endues violation have been met. These reports are a prime indicator of end-use and retransfer weaknesses within the end-use monitoring process for the involved country. Typically, the reports show that

unauthorized end-use occurrences tend to take place during the period after items are delivered. This tends to confirm that the greatest uncertainty in item control lies between the time the item is delivered to the foreign recipient and authorized disposal. This is the period during the life of each item when USG involvement is least direct and feedback on item status is least structured. It is therefore easily perceived as the weakest segment of the processes supporting EUM.

Based on AECA, Sec 40A, DoD instituted:

• "Post-delivery" standards were established which complement "Customer," "End-User," and "Shipment" pre-shipment controls established under Blue Lantern and discussed in a previous section of this chapter. Post-delivery standards are designed to highlight weaknesses which signal the need for added vigilance, most notably on the part of the country team, including the SAO, and by the end-user. The need for Post Delivery checks is indicated when:

There is any indication an AECA violation has occurred. These checks are normally confined to the indicated problem, but expand if a larger problem or weakness is found.

Substantial defense interaction or other ties are developing with countries whose interests are not compatible with those of the U.S. For example, the end-user holds relatively high technology U.S. items and also holds items from, or has defense relationships with, countries (1) not eligible for Foreign Military Sales (FMS) and other AECA and FAA programs (see SAMM Table 600-1), (2) for which AECA and FAA programs have been suspended for other than financial reasons, or (3) for which exports are proscribed (see ITAR Part 126.1).

Significant and unusual political or military upheaval is impending or has occurred. This includes unusual troop and equipment movements which could weaken normal accountability controls.

Countries unfriendly to the U.S. in the region are illicitly seeking U.S. equipment or support items of the types held by the end-user.

• Substantial problems or weaknesses are found during a GSOMIA security survey.

• Checks are mandatory at any time the DoS reports an AECA, Sec 3 violation, as follows:

• Within 60 calendar days after notification such a report has been made, SAOs within the involved country will initiate action to complete sample checks of at least two U.S.- origin items for each Sec 3 report. The SAO may personally conduct sample checks but assistance from other country team members, the supporting unified command, or from experienced counterparts within the host country can often facilitate a level of checks which would not be possible using SAO resources alone.

• Items selected for special checks will be those where receipt and subsequent accountability are representative of the item involved in the DoS report.

The primary purpose of the special checks is to gather additional information to ascertain or reconfirm the adequacy of the country accounting process. A secondary purpose is to determine if EUM problems exist for the specific items chosen. When the checks are performed, the SAO should be especially mindful of potential problems leading to the report which prompted the check. For example, transfer of an item to another country without DoS approval might result in a focus on:

- Areas where an accounting lapse may create conditions where the country defense establishment could lose item control,

- Training of personnel regarding EUM requirements and procedures, and

Practices regarding personnel or other actions related to deliberate or repeated loss of control.

The check should provide information for both the country and the U.S. to help determine if:

- The country's process is sound but failed due to unusual circumstances,

- The process is not given sufficient priority, or

- The country is supporting economic initiatives, defense interests, or other agendas which are not consistent with EUM requirements and, from a local perspective, outweigh those requirements.

While making the checks above, SAOs should be alert for unauthorized use of hardware items as well as information provided during training or in technical assistance support. This includes misuse of operation and maintenance, study, or production technical data.

Information gained during these special checks which could be useful in correcting the immediate problem or improving future end-use controls should be shared with DoS, DoD, and the unified command. Information obtained by any country team member indicating a violation of end-use or retransfer assurances in AECA (e.g., Annex C) or FAA transfer agreements should be reported to DoS.

Information gained outside channels accessible to the country team should be provided through the chain of command to the attention of PM/RSAT and PM/DTC, Department of State.

Annex A of Appendix 5

Acronyms

AA&E	Arms, Ammunition, and Explosives
AECA	Arms Export Control Act of 1976, as amended
DFARS	Defense Federal Acquisition Regulation Supplement (FAR supplement)
DoD	(U.S.) Department of Defense
DoS	(U.S.) Department of State
EUM	End-Use Monitoring
FAA	Foreign Assistance Act of 1961, as amended
FAR	Federal Acquisition Regulation
FMS	Foreign Military Sales
GSOMIA	General Security of Military Information Agreement
ITAR	International Traffic in Arms Regulation
LOA	(U.S.) Letter of Offer and Acceptance
MAPAD	Military Assistance Program Address Directory (DoD 4000.25-8-M)
MDE	Major Defense Equipment
MoD	Ministry of Defense (Non-U.S. DoD equivalent)
NAMSA	NATO Maintenance and Supply Agency
NATO	North Atlantic Treaty Organization
NDP	National Disclosure Policy
SAMM	Security Assistance Management Manual, DoD 5105.38-M
SAO	(U.S.) Security Assistance Office, (U.S.) Security Assistance Officer
SME	Significant Military Equipment
TTWG	Technology Transfer Working Group
U.S.	United States
USG	U.S. Government
USML	U.S. Munitions List

Annex B of Appendix 5

Sample AECA/FAA Presidential Determination

The White House
Washington

[date]

MEMORANDUM FOR THE SECRETARY OF STATE

SUBJECT: Eligibility of [country] to be Furnished Defense Articles and Services Under the Foreign Assistance Act and the Arms Export Control Act

Pursuant to the authority vested in me by section 503(1) of the Foreign Assistance Act of 1961, as amended (22 U.S.C. 2311(a)), and section 3(a)(1) of the Arms Export Control Act as amended (22 U.S.C. 2753(a)(1), I hereby find that the furnishing of defense articles and services to the Government of [country] will strengthen the security of the United States and promote world peace.

You are authorized and directed to report this finding to the Congress and to publish it in the Federal Register.

[Signature of the President]

Annex C of Appendix 5

LOA Security, End-Use, and Retransfer Provisions

The following terms are included in each United States of America Letter of Offer and Acceptance, the agreement through which countries purchase defense articles and services under authority of the AECA. Comparable provisions are incorporated into FAA section 505 agreements on which FAA programs are based.

(2.2) The Purchaser agrees, except as may otherwise be mutually agreed in writing, to use the defense articles sold hereunder only:

(2.2.1) For purposes specified in any Mutual Defense Assistance Agreement between the USG and the Purchaser;

(2.2.2) For purposes specified in any bilateral or regional defense treaty to which the USG and the Purchaser are both parties, if section 2.2.1 is inapplicable; or,

(2.2.3) For internal security, individual self-defense, or civic action, if sections 2.2.1 and 2.2.2 are inapplicable.

(2.3) The Purchaser will not transfer title to, or possession of, the defense articles, components, and associated support material, related training, or other defense services (including plans, specifications, or information), or technology furnished under this LOA to anyone who is not an officer, employee, or agent of the Purchaser (excluding transportation agencies) and shall not use or permit their use for purposes other than those authorized, unless the written consent of the USG has first been obtained. The Purchaser will ensure, by all means available to it, respect for proprietary rights in any items and any plans, specifications, or information furnished, whether patented or not. The Purchaser also agrees that the defense articles offered will not be transferred to Cyprus or otherwise used to further the severance or division of Cyprus and recognizes that the U.S. Congress is required to be notified of any substantial evidence that the defense articles sold in this LOA have been used in a manner which is inconsistent with this provision.

(2.4) To the extent that items, including plans, designs, specifications, technical data, or information, furnished in connections with this LOA may be classified by the USG for security purposes, the Purchaser certifies that it will maintain a similar classification and employ measures necessary to preserve such security, equivalent to those employed by the USG and commensurate with security agreements between the USG and the Purchaser. If such security agreements do not exist, the Purchaser certifies that classified items will be provided only to those individuals having an adequate security clearance and a specific need to know in order to carry out the LOA program and that it will promptly and fully inform the USG of any compromise or possible compromise of U.S. classified material or information furnished pursuant to this LOA. The Purchaser further certifies that if a U.S. classified item is to be furnished to its contractor pursuant to this LOA: (a) items will be exchanged through official government channels, (b) the specified contractor has been granted a facility security clearance by the Purchaser at a level at least equal to the classification level of the U.S. information involved, (c) all contractor personnel requiring access to such items have been cleared to the appropriate level by the Purchaser, and (d) the Purchaser will assume responsibility for administering security measures while in the contractor's possession. If a commercial transportation agent is to be used for shipment, the Purchaser certifies that such agent has been cleared at the appropriate level for handling classified items. These measures will be maintained throughout the period during which the USG may maintain such

classification. The USG will use its best efforts to notify the Purchaser if the classification is changed.

Annex D of Appendix 5

General Security of Military Information Agreement

The following is a typical GSOMIA, developed for the U.S. under National Disclosure Policy by the National Disclosure Policy Committee, chaired by DoD. Each agreement is developed to provide overall protections for U.S. classified military information provided to other countries and for classified information entrusted by those countries to the United States. Bandaria is unrelated to any actual country, past or present.

AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED STATES OF AMERICAAND THE GOVERNMENT OF BANDARIA CONCERNING MEASURES FOR THE PROTECTION OF CLASSIFIED MILITARY INFORMATION

The Government of the United States of America and the Government of Bandaria (hereinafter the Parties), in furtherance of mutual cooperation and to ensure the protection of classified military information provided by either party to the other, have agreed as follows:

Article 1
Applicability

A. Classified military information provided directly or indirectly by one Party to the other Party, or to an officer or other representative of one of the Parties, shall be protected in accordance with the laws and regulations of the Parties and the terms set forth herein.

B. The Parties shall promptly notify each other of any changes to their laws and regulations that would affect the protection of classified military information under this Agreement. In such case, the Parties shall consult, as provided for in Article 15, to consider possible changes to this Agreement.

C. For the purpose of this Agreement, classified military information is information that is generated by or for the Department of Defense of the United States of America or by or for the Ministry of National Defense of Bandaria, or that is under their jurisdiction or control, and which requires protection in the interests of national security of the Parties. For the United States of America, this information is marked CONFIDENTIAL, SECRET, or TOP SECRET. For Bandaria, it is marked CONFIDENCIAL, SECRETO, and ULTRA SECRETO. The United States will treat Bandarian CONFIDENCIAL and SECRETO information as U.S. SECRET information and will treat Bandarian ULTRA SECRETO as U.S. TOP SECRET. Bandaria will treat United States of America CONFIDENTIAL as Bandarian CONFIDENCIAL, U.S. SECRET as Bandarian SECRETO, and U.S. TOP SECRET as Bandarian ULTRA SECRETO information. The information may be in oral, visual, or documentary form, or in the form of equipment or technology.

Article 2
Implementing Agencies

For the Government of the United States of America, the implementing agency shall be the Department of Defense. For the Government of Bandaria, the implementing agency shall be the Ministry of National Defense. Supplemental agreements under this Agreement may be concluded by the designated implementing agencies in accordance with this Agreement.

Article 3
Access

No individual shall be entitled to access to the information covered by this Agreement solely by virtue of rank, appointment, or security clearance. Access to the information shall be granted only to those individuals whose official duties require such access and who have been granted a personnel security clearance in accordance with the prescribed standards of the Parties. The Parties shall ensure that:

- The recipient Party will not release the information to a third-country government, person, or other entity of a third country without the prior written approval of the releasing Party;

- The recipient Party will afford the information a degree of protection equivalent to that afforded it by the releasing Party;

- The recipient Party will not use the information for other than the purpose for which it was provided without a prior written approval of the releasing Party;

- The recipient Party will respect private rights, such as patents, copyrights, or trade secrets which are involved in the information; and

- Each facility or establishment that handles classified military information shall maintain a registry of individuals at the facility or establishment who are authorized to have access to such information.

Article 4
Personnel Security

The determination on the granting of a personnel security clearance to an individual who will have access to information under this Agreement shall be consistent with the interests of national security of each Party and shall be based upon all available information indicating whether the individual is of unquestioned loyalty, integrity, and trustworthiness, and excellent character, and of such habits and associates as to cast no doubt upon his or her discretion or good judgment in the handling of classified information.

An appropriate investigation, in sufficient detail to provide assurance that the above criteria have been met, shall be conducted by the Parties with respect to any individual to be granted access to classified information covered by this Agreement.

Before any officer or a representative of a Party releases classified military information to an officer or representative of the other Party, the receiving Party shall provide to the releasing Party an assurance that the officer or representative possesses the necessary level of security clearance and requires access for official purposes, and that the information will be protected by the receiving Party according to the provisions of this Agreement.

Article 5
Visits

Authorizations for visits by representatives of one Party to facilities and establishments of the other Party, where access to classified military information is required, shall be limited to those necessary for official purposes. Authorizations to visit the facilities and establishments shall be granted only by government officials designated by the Parties. The Party to be visited or its

designee shall be responsible for advising the facility or establishment of the proposed visit, and the scope and highest level of classified information that may be furnished to the visitors.

Requests for visits to facilities and establishments in Bandaria shall be submitted through the United States Defense Attaché Office in Bandaria City

Requests for visits to facilities and establishments in the United States of America shall be submitted through the Bandarian Defense Attaché Office in Washington.

Article 6
Physical Security

The Parties shall be responsible for the physical security of all classified military information of the other Party while in transit or storage within their territory.

The Parties shall be responsible for the security of all government and private facilities and establishments where the information of the other Party is available and shall assure that qualified individuals are appointed for each such facility or establishment who shall have the responsibility and authority for the control and protection of the information.

The information shall be stored in a manner that assures access only by those individuals who have been authorized access pursuant to Article 3 of this Agreement.

Article 7
Transmission

Classified military information shall be transmitted between the Parties through government-to-government channels.

The minimum requirements for the security of the information during national or international transmission of classified military information shall be as follows:

(1) Documents and other media:

(a) Documents and other media containing classified military information shall be transmitted in double sealed envelopes, the innermost envelope bearing only the classification of the documents and the organizational address of the intended recipient and the outer envelope bearing the organizational address of the recipient, the organizational address of the sender, and the registry number, if applicable.

(b) No indication of the classification of the enclosed information shall be made on the outer envelope or wrapping.

(c) The sealed envelope shall be transmitted according to the prescribed regulations and procedures of the releasing Party.

(d) The Parties shall confirm in writing the receipt of the packages as well as the enclosed classified military information that are transferred between them.

(2) Equipment:

(a) Classified equipment shall be transported in sealed covered vehicles, or be securely packaged or protected, and kept under continuous control to prevent access by unauthorized persons.

(b) Classified equipment which must be stored temporarily awaiting shipment shall be placed in a secure, locked storage area. The area shall be protected by intrusion-detection equipment and/or guards who shall maintain continuous surveillance of the storage area. Only authorized personnel with the requisite security clearance shall have access to the storage area.

(c) Written confirmation shall be obtained on every occasion when classified equipment changes hands en route; and, a receipt shall be signed by the final recipient and returned to the sender.

(3) Electronic transmissions:

Classified military information transmitted by electronic means shall be encrypted.

Article 8
Accountability and Control

Accountability and control procedures shall be established to manage the dissemination of and access to classified military information covered by this Agreement.

Article 9
Marking of Documents

Each Party shall stamp or mark the name of the originating government on all classified military information received from the other Party. The information shall be marked with a national security classification marking of the recipient Party that will afford a degree of protection equivalent to that afforded to it by the releasing Party.

Article 10
Destruction

Classified documents and other media containing classified military information shall be destroyed by burning, shredding, pulping, or other means so as to prevent reconstruction of the classified information contained therein.

Also, classified equipment shall be destroyed beyond recognition or modified so as to preclude reconstruction of the classified military information in whole or in part.

Article 11
Reproduction

When documents or other media containing classified military information are reproduced, all original security markings thereon shall be reproduced or marked on each copy.

Such reproduced documents or media shall be placed under the same controls as the original document or media. The number of copies shall be limited to that required for official purposes.

Article 12
Translation

All translations of classified military information shall be made by individuals with security clearances pursuant to Article 4. The number of copies shall be kept to a minimum and the distribution thereof shall be controlled. Such translations shall bear appropriate security classification markings and a suitable notation in the language into which it is translated; indicating that the documents or other media contain classified military information of the releasing Party.

Article 13
Release To Contractors

Prior to the release to a contractor or prospective contractor of any classified military information covered by this Agreement received from the other Party, the recipient Party shall:

Ensure that such contractor or prospective contractor and the contractor's facility have the capability to protect the information;

Grant to the facility an appropriate facility security clearance;

Grant appropriate personnel security clearances for those individuals whose duties require access to the information;

Ensure that all individuals having access to the information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations;

Carry out periodic security inspections of cleared facilities to ensure that the information is protected as required herein; and

Ensure that access to the information is limited to those persons who have a need to know for official purposes.

Article 14
Action in the Event of Loss or compromise or Possible Loss or Compromise

The releasing Party shall be informed immediately of all losses or compromises, as well as possible losses or compromises, of its classified military information, and the recipient party shall initiate an investigation to determine the circumstances. The results of the investigation and information regarding measures taken to prevent recurrence shall be forwarded to the releasing Party by the Party that conducts the investigation.

Article 15
Review of Security Systems

Implementation of the foregoing security requirements can be advanced through reciprocal visits by security personnel of the Parties. Accordingly, security representatives of the Parties, after prior consultation, shall be permitted to visit the other Party, to discuss, and view firsthand, the implementing procedures of the other Party in the interest of achieving reasonable comparability of the security systems. Each Party shall assist the security representatives in determining whether classified military information provided by the other Party is being adequately protected.

Article 16
Implementation and Termination

This Agreement shall enter into force on the date of last notification that all legal procedures of both Parties have been met.

This Agreement shall remain in force for a period of five years and shall be extended automatically annually thereafter, unless either Party notifies the other in writing, ninety days in advance, of its intention to terminate the Agreement.

Notwithstanding the termination of this Agreement, all classified military information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

DONE at Washington DC this 5th day of January 1997, in duplicate, in the English and Bandarian languages, both texts being equally authentic.

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA:	FOR THE GOVERNMENT OF BANDARIA:
[Signature of the Secretary of Defense]	[Signature of the Minister of National Defense]

Annex E of Appendix 5
Evolution of a Country Program

Based on assessments in the early stages of U.S.-country relationships, it may be determined that cooperative defense programs would be of mutual benefit. A typical program might evolve as follows:

- A formal assessment, culminating with a Presidential Determination (see Annex B) sets the stage for AECA and FAA programs.

- The DoS approves a few small country programs. For example, one AECA program might authorize DoD to initiate an LOA for a training course, including instruction on military support to civilian leaders in a democratically elected government, to a few carefully selected military officers. Another program may authorize DoD to develop an LOA for 2,000 serviceable excess military uniforms from DoD stocks. Within government programs, core agreements and procedures apply for transfer of any item under the AECA and FAA, including training courses and uniforms. Countries are therefore introduced to end-use control responsibilities at the earliest stages of government programs. Because items may not be included on the U.S. Munitions List (USML, see SAMM chapter 2), commercial sales for the same items may require virtually no export or end-use controls.

- Several years pass, contacts continue, and other programs are approved and implemented. During a joint exercise, the country minister of defense (MoD) finds U.S. mobility is superior to his own and, after obtaining information on possible options, further study, coordination within his own government, and consultation with U.S. representatives in country and in the United States, provides a letter of request to the local U.S. embassy for ten utility helicopters. The embassy adds its assessment of impact on regional arms balances, country ability to absorb the aircraft into its force structure, and other information, including a recommendation of approval or disapproval. The request is provided to DoD, with a copy to DoS. While DoD starts action to offer to sell the items, DoS completes its own assessment and disapproves the sale, halting work by DoD, or approves and allows the sales offer process to continue. Prior to release, each offer must be cleared by DoS, ensuring that no sales offers are made without approval of that Department. During the course of developing the offer, DoD checks to determine if the helicopters, including related items such as night vision equipment, armaments, training, or technical publications, exceed the levels of sensitivity authorized for transfer to the country. If so, this issue is considered in a DoD-DoS interagency National Disclosure Policy process (see the section labeled Sensitive Item Control) and the results are factored into the ultimate release decision. The helicopters are Significant Military Equipment (SME) on the USML of the International Traffic in Arms Regulation (ITAR), and have been designated as major defense equipment (MDE). Both DoS and Congress are therefore involved in actions leading up to the formal Congressional notification under AECA, Sec 36(b) preceding clearance by DoS and release of the LOA to the requesting country.

- A country MoD representative signs the offer for the country, which includes the agreement for end-use and retransfer (see Annex C), which is crafted to comply with AECA, Sec 3(a). Simultaneously with return of the signed LOA, the country provides funds for the helicopters and related items offered. DoD initiates action leading to contract award and administers the contract under federal acquisition policies and procedures. Following LOA implementation, award of contracts, and production, all defense articles are delivered. Services, primarily pilot and maintenance training, are completed concurrently. Several months before delivery of the helicopters, an LOA is requested, processed, and accepted for supply of spare parts, in anticipation of maintenance needs. Another LOA is accepted in anticipation of the need for ongoing technical support, including repair services which are beyond in-country capability,

replacement pilot and crew chief training, and safety of flight and other modifications. To reduce risk of damage during delivery, the original LOA includes transportation services whereby the aircraft are moved to country by U.S. military airlift and released to the authorized representative of the MoD. As non-sensitive repair parts from the original and follow-on LOAs become available, they are delivered to the country's U.S. corporation freight forwarder for onward movement to the country. A classified night vision item, door-mounted machine-guns and ammunition, and other sensitive items are delivered through the Defense Transportation System. This provides normal DoD security to the point of release to a MoD representative in the end-user country.

- The SAO, part of the U.S. in-country team led by the ambassador, has been assisting the MoD throughout the program. The SAO works with country military counterparts to ensure accounting processes have been established to protect against use contrary to the transfer agreement. The SAO monitors the helicopter and other FAAand AECA programs under authority of FAA, Sec 515; the SAMM (see Chapters 4 and 11); and other guidance directly from DoD, through the country team from DoS, and from the unified commander for his region. The SAO is alert for accounting weaknesses and brings those and any other indications of end-use or retransfer problems to the attention of country counterparts. If not satisfactorily resolved, these problems are raised for resolution through the chain of command within the country team. If not resolvable by the country team, they are raised to DoS for resolution.

- Procedures imposed for shipments to DoD units are generally used for providing status and receiving feedback to track item movement for AECA and FAA programs. Discrepancy reports are submitted by country representatives for items found to be missing or damaged at the time of receipt. When entire shipments, including transportation documents, are not received, discrepancy reports are submitted based on the bills provided subsequent to each DoD shipment. These discrepancy reports complement other shipment documentation to ensure items released by DoD are received at the proper destination.